Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (original) An apparatus comprising:

a configuration storage containing configuration parameters to configure an access transaction generated by a processor having a normal execution mode and an isolated execution mode, the access transaction having access information; and

an access checking circuit coupled to the configuration storage to check the access transaction using at least one of the configuration parameters and the access information.

2. (original) The apparatus of claim 1 wherein the configuration parameters include an isolated setting and an execution mode word.

3. (original) The apparatus of claim 2 wherein the access information comprises a physical address and an access type, the access type indicating if the access transaction is one of a memory access, an input/output access, and a logical processor access, the physical address being one of a translation lookaside buffer (TLB) physical address from a TLB and a front side bus (FSB) physical address from an FSB.

4. (original) The apparatus of claim 3 wherein the configuration storage comprises:

a setting storage to contain the isolated setting for defining an isolated memory area corresponding to a memory external to the processor.

5. (original) The apparatus of claim 4 wherein the setting storage comprises:

a base register, a mask register, and a length register to store a base value, a mask value, and a length value, respectively, a combination of at least two of the base, mask, and length values forming the isolated setting.

6. (original) The apparatus of claim 5 wherein the configuration storage further comprises:

a processor control register to contain the execution mode word, the execution mode word being asserted when the processor is configured in the isolated execution mode.

7. (currently amended) The apparatus of claim 6 wherein the access checking circuit comprises:

TLB and FSB address detectors to detect if the TLB and FSB physical addresses are within the isolated memory area defined by the isolated setting, the TLB and FSB ~~the~~ address detectors generating a processor isolated access signal and an FSB isolated access signal, respectively.

8. (original) The apparatus of claim 7 wherein the access checking circuit further comprises:

a snoop checking circuit coupled to a cache and the address detector to generate a processor snoop access signal.

9. (original) The apparatus of claim 8 wherein the snoop checking circuit comprises:

a snoop combiner to combine a cache access signal, the FSB isolated access signal, and an external isolated access signal from another processor, the combined cache access signal, the processor isolated access signal and the external isolated access signal corresponding to the processor snoop access signal.

10. (original) The apparatus of claim 7 wherein the access checking circuit further comprises:

an access grant generator coupled to the address detector and the processor control register to generate an access grant signal indicating if the access transaction is valid.

11. (original) The apparatus of claim 7 wherein the logical processor access is one of a logical processor entry and a logical processor exit.

12. (original) The apparatus of claim 11 wherein the access checking circuit comprises:

a logical processor manager to manage a logical processor operation caused by the logical processor access.

13. (original) The apparatus of claim 12 wherein the logical processor manager comprises:

a logical processor register to store a logical processor count indicating a number of logical processors currently enabled;

a logical processor state enabler to enable a logical processor state when the logical processor access is valid;

a logical processor updater coupled to the logical processor register to update the logical processor count according to the logical processor access, the logical processor updater being enabled by the enabled logical processor state;

a minimum detector coupled to the logical processor register to determine if the logical processor count is equal to a minimum logical processor value; and

a maximum detector coupled to the logical processor register to determine if the logical processor count exceeds a maximum logical processor value.

14. (original) The apparatus of claim 13 wherein the logical processor updater initializes the logical processor register when there is no enabled logical processor.

15. (original) The apparatus of claim 14 wherein the logical processor updater updates the logical processor count in a first direction when the access transaction corresponds to the logical processor entry, and updates the logical processor count in a second direction opposite to the first direction when the access transaction corresponds to the logical processor exit.

16. (original) A method comprising:

configuring an access transaction generated by a processor by a configuration storage containing configuration parameters, the processor having a normal execution mode and an isolated execution mode, the access transaction having access information; and

checking the access transaction by an access checking circuit using at least one of the configuration parameters and the access information.

17. (original) The method of claim 16 wherein the configuration parameters include an isolated setting and an execution mode word.

18. (original) The method of claim 17 wherein the access information comprises a physical address and an access type, the access type indicating if the access transaction is one of a memory access, an input/output access, and a logical processor access, the physical address being one of a translation lookaside buffer (TLB) physical address from a TLB and a front side bus (FSB) physical address from an FSB.

19. (original) The method of claim 18 wherein configuring the access transaction comprises:

defining an isolated memory area corresponding to a memory external to the processor by the isolated setting contained in a setting storage.

20. (original) The method of claim 19 wherein defining the isolated memory area comprises:

forming the isolated setting by a combination of at least two of a base value, a mask value, and a length value stored in a base register, a mask register, and a length register, respectively.

21. (original) The method of claim 20 wherein configuring the access transaction further comprises:

asserting the execution mode word stored in a processor control register when the processor is configured in the isolated execution mode.

22. (original) The method of claim 21 wherein checking the access transaction comprises:

detecting if the TLB and FSB physical addresses are within the isolated memory area defined by the isolated setting by TLB and FSB address detectors, respectively, the TLB and FSB address detectors generating processor and FSB isolated access signals, respectively.

23. (original) The method of claim 22 wherein checking the access transaction further comprises:

generating a processor snoop access signal by a snoop checking circuit.

24. (original) The method of claim 23 wherein generating the processor snoop access signal comprises:

combining a cache access signal, the FSB isolated access signal, and an external isolated access signal from another processor by a snoop combiner, the combined cache access signal, the processor isolated access signal and the external isolated access signal corresponding to the processor snoop access signal.

25. (original) The method of claim 22 wherein checking the access transaction further comprises:

generating an access grant signal indicating if the access transaction is valid by an access grant generator.

26. (original) The method of claim 22 wherein the logical processor access is one of a logical processor entry and a logical processor exit.

27. (original) The method of claim 26 wherein checking the access transaction comprises:

managing a logical processor operation caused by the logical processor access by a logical processor manager.

28. (original) The method of claim 27 wherein managing the logical processor operation comprises:

storing a logical processor count indicating a number of logical processors currently enabled in a logical processor register;

enabling a logical processor state when the logical processor access is valid by a logical processor state enabler;

updating the logical processor count according to the logical processor access by a logical processor updater, the logical processor updater being enabled by the enabled logical processor state;

determining if the logical processor count is equal to a minimum logical processor value by a minimum detector; and

determining if the logical processor count exceeds a maximum logical processor value by a maximum detector.

29. (original) The method of claim 28 wherein updating the logical processor count comprises:

initializing the logical processor register when there is no enabled logical processor.

30. (original) The method of claim 29 wherein updating the logical processor count comprises:

updating the logical processor count in a first direction when the access transaction corresponds to the logical processor entry; and

updating the logical processor count in a second direction opposite to the first direction when the access transaction corresponds to the logical processor exit.

31. (original) A system comprising:

a chipset;

a memory coupled to the chipset having an isolated memory area; and

a processor coupled to the chipset and the memory having an access manager, the processor having a normal execution mode and an isolated execution mode, the processor generating an access transaction having access information, the access manager comprising:

a configuration storage containing configuration parameters to configure the access transaction, and

an access checking circuit coupled to the configuration storage to check the access transaction using at least one of the configuration parameters and the access information.

32. (original) The system of claim 31 wherein the configuration parameters include an isolated setting and an execution mode word.

33. (original) The system of claim 32 wherein the access information comprises a physical address and an access type, the access type indicating if the access transaction is one of a memory access, an input/output access, and a logical processor access, the physical address being one of a translation lookaside buffer (TLB) physical address from a TLB and a front side bus (FSB) physical address from an FSB.

34. (original) The system of claim 33 wherein the configuration storage comprises:

a setting storage to contain the isolated setting for defining the isolated memory area.

35. (original) The system of claim 34 wherein the setting storage comprises:

a base register, a mask register, and a length register to store a base value, a mask value, and a length value, respectively, a combination of at least two of the base, mask, and length values forming the isolated setting.

36. (original) The system of claim 35 wherein the configuration storage further comprises:

a processor control register to contain the execution mode word, the execution mode word being asserted when the processor is configured in the isolated execution mode.

37. (original) The system of claim 36 wherein the access checking circuit comprises:

TLB and FSB address detectors to detect if the TLB and FSB physical addresses are within the isolated memory area defined by the isolated setting, respectively, the TLB and FSB address detectors generating a processor isolated access signal and an FSB isolated access signal, respectively.

38. (original) The system of claim 37 wherein the access checking circuit further comprises:

a snoop checking circuit coupled to a cache and the address detector to generate a processor snoop access signal.

39. (original) The system of claim 38 wherein the snoop checking circuit comprises:

a snoop combiner to combine a cache access signal, the FSB isolated access signal, and an external isolated access signal from another processor, the combined cache access signal, the processor isolated access signal and the external isolated access signal corresponding to the processor snoop access signal.

40. (original) The system of claim 37 wherein the access checking circuit further comprises:

an access grant generator coupled to the address detector and the processor control register to generate an access grant signal indicating if the access transaction is valid.

41. (original) The system of claim 37 wherein the logical processor access is one of a logical processor entry and a logical processor exit.

42. (original) The system of claim 41 wherein the access checking circuit comprises:

a logical processor manager to manage a logical processor operation caused by the logical processor access.

43. (original) The system of claim 42 wherein the logical processor manager comprises:

a logical processor register to store a logical processor count indicating a number of logical processors currently enabled;

a logical processor state enabler to enable a logical processor state when the logical processor access is valid;

a logical processor updater coupled to the logical processor register to update the logical processor count according to the logical processor access, the logical processor updater being enabled by the enabled logical processor state;

a minimum detector coupled to the logical processor register to determine if the logical processor count is equal to a minimum logical processor value; and

a maximum detector coupled to the logical processor register to determine if the logical processor count exceeds a maximum logical processor value.

44. (original) The system of claim 43 wherein the logical processor updater initializes the logical processor register when there is no enabled logical processor.

45. (original) The system of claim 44 wherein the logical processor updater updates the logical processor count in a first direction when the access transaction corresponds to the logical processor entry, and updates the logical processor count in a second direction opposite to the first direction when the access transaction corresponds to the logical processor exit.

46. (original) A computer program product comprising:

a machine readable medium having computer program code embodied therein, the computer program product having:

computer readable program code for configuring an access transaction generated by a processor by a configuration storage containing configuration parameters, the processor having a normal execution mode and an isolated execution mode, the access transaction having access information; and

computer readable program code for checking the access transaction by an access checking circuit using at least one of the configuration parameters and the access information.

47. (original) The computer program product of claim 46 wherein the configuration parameters include an isolated setting and an execution mode word.

48. (original) The computer program product of claim 47 wherein the access information comprises a physical address and an access type, the access type indicating if the access transaction is one of a memory access, an input/output access, and a logical processor access, the physical address being one of a translation lookaside buffer (TLB) physical address from a TLB and a front side bus (FSB) physical address from an FSB.

49. (original) The computer program product of claim 48 wherein the computer readable program code for configuring the access transaction comprises:

computer readable program code for defining an isolated memory area corresponding to a memory external to the processor by the isolated setting contained in a setting storage.

50. (original) The computer program product of claim 49 wherein the computer readable program code for defining the isolated memory area comprises:

computer readable program code for forming the isolated setting by a combination of at least two of a base value, a mask value, and a length value stored in a base register, a mask register, and a length register, respectively.

51. (original) The computer program product of claim 50 wherein the computer readable program code for configuring the access transaction further comprises:

computer readable program code for asserting the execution mode word stored in a processor control register when the processor is configured in the isolated execution mode.

52. (original) The computer program product of claim 51 wherein the computer readable program code for checking the access transaction comprises:

computer readable program code for detecting if the TLB and FSB physical addresses are within the isolated memory area defined by the isolated setting by TLB and FSB address detectors, respectively, the TLB and FSB address detectors generating processor and FSB isolated access signals, respectively.

53. (original) The computer program product of claim 52 wherein the computer readable program code for checking the access transaction further comprises:

computer readable program code for generating a processor snoop access signal by a snoop checking circuit.

54. (original) The computer program product of claim 53 wherein the computer readable program code for generating the processor snoop access signal comprises:

computer readable program code for combining a cache access signal, the FSB isolated access signal, and an external isolated access signal from another processor by a snoop combiner, the combined cache access signal, the processor isolated access signal and the external isolated access signal corresponding to the processor snoop access signal.

55. (original) The computer program product of claim 52 wherein the computer readable program code for checking the access transaction further comprises:

computer readable program code for generating an access grant signal indicating if the access transaction is valid by an access grant generator.

56. (original) The computer program product of claim 52 wherein the logical processor access is one of a logical processor entry and a logical processor exit.

57. (original) The computer program product of claim 56 wherein the computer readable program code for checking the access transaction comprises:

computer readable program code for managing a logical processor operation caused by the logical processor access by a logical processor manager.

58. (original) The computer program product of claim 57 wherein the computer readable program code for managing the logical processor operation comprises:

computer readable program code for storing a logical processor count indicating a number of logical processors currently enabled in a logical processor register;

computer readable program code for enabling a logical processor state when the logical processor access is valid by a logical processor state enabler;

computer readable program code for updating the logical processor count according to the logical processor access by a logical processor updater, the logical processor updater being enabled by the enabled logical processor state;

computer readable program code for determining if the logical processor count is equal to a minimum logical processor value by a minimum detector; and

computer readable program code for determining if the logical processor count exceeds a maximum logical processor value by a maximum detector.

59. (original) The computer program product of claim 58 wherein the computer readable program code for updating the logical processor count comprises:

computer readable program code for initializing the logical processor register when there is no enabled logical processor.

60. (original) The computer program product of claim 59 wherein the computer readable program code for updating the logical processor count comprises:

computer readable program code for updating the logical processor count in a first direction when the access transaction corresponds to the logical processor entry; and

computer readable program code for updating the logical processor count in a second direction opposite to the first direction when the access transaction corresponds to the logical processor exit.